UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/815,572	03/31/2004	Ilya Mironov	MS1-1921US	9406

22801 7590 04/30/2008

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
PAN, JOSEPH T	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
04/30/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/815,572	MIRONOV ET AL.	
	Examiner	Art Unit	
	JOSEPH PAN	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 January 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-40* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-40* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *31 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's response filed on January 8, 2008 has been carefully considered. Claims 31 and 38 have been amended. Claims 1-40 are pending.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-10, 13-25, 28-37, 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Reeds, III (U.S. Patent No. 5,724,427), hereinafter "Reeds", in view of Greene et al. (U.S. Patent No. 6,646,639 B1), hereinafter "Greene", and further in view of Bitterlich et al. (U.S. Patent No. 7,230,978 B2), Hereinafter "Bitterlich".

Referring to claims 1, 18, 31:

i. Reeds teaches:

A method comprising:

sequentially storing a plurality of results provided by a stream cipher output rule in a first, second, and third storage units (see figure 3; column 7, lines 20-31; and column 8, lines 12-18 of Reeds);

providing a plurality of results from a pairing function, the pairing function pairing individual values from the first and third storage units that are at least a threshold value apart (see figure 3; column 7, lines 20-31; and column 8, lines 12-18 of

Reeds); and

upon reaching the threshold value of the output rule results, serially rotating contents of the first, second, and third storage units (see figure 3; column 7, lines 20-31; and column 8, lines 12-18 of Reeds).

However, Reeds does not specifically mention the threshold value.

Reeds discloses storing the result of the encryption processor to a rotational state vector (see figure 3, element 320, 'Text c', 'rotational state vector', of Reeds). However, Reeds does not specifically mention storing the result into output buffers, such as a first, second, third storage units.

ii. Greene teaches a method for improved occlusion clustering in graphics systems wherein Greene disclose using the threshold value to determine whether to perform an arithmetic operation (see figure 13, elements 1338, 1342; column 24, line 57-59; and column 25, lines 10-15 '...new coefficients for the polygon's edge and plane equations', of Greene).

Bitterlich teaches a reconfigurable channel CODEC (encoder and decoder) processor for a wireless communication system where in Bitterlich discloses the output buffer (see column 7, lines 19-27 "The memories 202 and 242 can be used to communicate data between processor cores and also serve as a central CODEC "bulk storage." A typical application within the field of communication devices in general and for the channel CODEC in particular is the use of these central memories for implementation of large **input/output** FIFO **buffers**, **double/triple or general rotating buffering schemes** and for the relatively large interleaving/de-interleaving buffers.", of Bitterlich, emphasis added).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Greene into the method of Reeds to use a threshold value to determine whether to perform an arithmetic operation.

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Bitterlich into the method of

Reeds to use the central memories for implementation of large input/output FIFO buffers, double/triple or general rotating buffering schemes.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Greene into the system of Reeds to use a threshold, because Reeds teaches performing arithmetic operations on a rotational state vector (see figure 3, element 310 'rotational state vector'; and column 5, lines 48-53 'In particular, the method may be used as a stream cipher in which one or more values of elements in a rotational state vector, used to encrypt a plain byte to yield a cipher text byte, are changed as a function of one or more of: the cipher text byte or the plain text byte.', Reeds, emphasis added), and Greene teaches use a threshold value to determine whether to perform an arithmetic operation. Therefore, Greene's teaching could enhance Reeds' system.

The ordinary skilled person would have been motivated to have applied the teaching of Bitterlich into the system of Reeds to use the central memories for implementation of large input/output FIFO buffers, double/triple or general rotating buffering schemes, because Reeds teaches storing the result of the encryption processor to a rotational state vector (see figure 3, element 320, 'Text c', 'rotational state vector', of Reeds). Bitterlich teaches ""The memories 202 and 242 can be used to communicate data between processor cores and also serve as a central CODEC "bulk storage." A typical application within the field of communication devices in general and for the channel CODEC in particular is the use of these central memories for implementation of large **input/output** FIFO **buffers**, **double/triple or general rotating buffering schemes** and for the relatively large interleaving/de-interleaving buffers." (see column 7, lines 19-27 of Reeds). Therefore, Bitterlich's teaching could enhance Reeds' system.

Referring to claims 2, 19, 32:

Reeds, Greene, and Bitterlich disclose the claimed subject matter: a stream ciphering method (see claim 1 above). They further disclose the correlation (see column 41, lines 60-61 of Greene).

Referring to claims 3, 20, 33:

Reeds, Greene, and Bitterlich disclose the claimed subject matter: a stream ciphering method (see claim 1 above). They further disclose the threshold value (see column 24, line 58 of Greene).

Referring to claims 4, 21, 34:

Reeds, Greene, and Bitterlich disclose the claimed subject matter: a stream ciphering method (see claim 1 above). They further disclose the first, second and third storage units (see column 8, lines 12-18 of Reeds), and memory device (see column 7, line 15 of Reeds).

Referring to claim 5, 22, 35:

Reeds, Greene, and Bitterlich disclose the claimed subject matter: a stream ciphering method (see claim 1 above). They further disclose the shifting (see column 27, lines 10-18 of Greene).

Referring to claims 6, 23, 36:

Reeds, Greene, and Bitterlich disclose the claimed subject matter: a stream ciphering method (see claim 1 above). They further disclose the pairing (see column 5, lines 22-23 of Greene), and the table (see column 7, line 10 of Reeds).

Referring to claims 7, 24:

Reeds, Greene, and Bitterlich disclose the claimed subject matter: a stream ciphering method (see claim 1 above). They further disclose the stream cipher keystream generator (see figure 3; and column 7, lines 20-31 of Reeds).

Referring to claims 8, 25:

Reeds, Greene, and Bitterlich disclose the claimed subject matter: a stream ciphering method (see claim 1 above). They further disclose the first and third storage units (see column 8, lines 12-18 of Reeds).

Referring to claims 9, 16, 29:

Reeds, Greene, and Bitterlich disclose the claimed subject matter: a stream ciphering method (see claim 1 above). They further disclose the initialization (see column 5, line 58 of Reeds).

Referring to claims 17, 30:

Reeds, Greene, and Bitterlich disclose the claimed subject matter: a stream ciphering method (see claim 1 above). They further disclose the delay (see column 42, line 12 of Greene).

Referring to claims 10, 37:

Reeds, Greene, and Bitterlich disclose the claimed subject matter: a stream ciphering method (see claim 1 above). They further disclose the recursive algorithm (see column 3, line 13 of Greene).

Referring to claims 13-14, 28, 40:

Reeds, Greene, and Bitterlich disclose the claimed subject matter: a stream ciphering method (see claim 1 above). They further disclose the fourth storage unit (see column 8, lines 12-18 of Reeds).

Referring to claim 15:

Reeds, Greene, and Bitterlich disclose the claimed subject matter: a stream ciphering method (see claim 1 above). They further disclose the permutation (see column 9, line 46 of Reeds).

4. Claims 11-12, 26-27, 38-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Reeds, III (U.S. Patent No. 5,724,427) in view of Greene et al. (U.S. Patent No. 6,646,639 B1), and further in view of Bitterlich et al. (U.S. Patent No. 7,230,978 B2), and further in view of Petersen et al. (U.S. Patent No. 7,170,997 B2), hereinafter "Petersen".

Referring to claims 11-12, 26-27, 38-39:

i. Reeds, Greene, and Bitterlich disclose the claimed subject matter: a stream ciphering method (see claim 1 above). They further disclose the update rule (see column 50, lines 6-10 of Greene).

However, they do not specifically mention the random walk.

ii. Petersen teaches a method of performing numerical computation wherein Petersen discloses the random walk (see column 41, lines 48-49; and column 42, lines 3-9 of Petersen).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Petersen into the method of Reeds, Greene, and Bitterlich to utilize the random walk.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Petersen into the system of Reeds, Greene, and Bitterlich to utilize the random walk, because Reeds and Greene teach the updating rule (see column 50, lines 6-10 of Greene), and "In this test, the sequence is similarly to the cumulative sums test transferred into a random walk. The number of visits to certain states (values the cumulative sum can hold), which the random walk potentially passes through, is used to characterize the sequence as either random or non-random." (see column 42, lines 3-9 of Petersen).

Response to Arguments

5. Applicant's arguments, filed on January 8, 2008, have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Bitterlich.

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Joseph Pan whose telephone number is 571-272-5987.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

Joseph Pan
April 23, 2008
/KIMYEN VU/

Supervisory Patent Examiner, Art Unit 2135